



## **PRIVACY IMPACT ASSESSMENT**

### **INTRODUCTION**

The objective of the Privacy Impact Analysis (PIA) is to determine the scope, justification, and Privacy Act applicability for systems collecting, storing or processing sensitive, personal data that may be considered private. Upon completion of the questionnaire and acquisition of signatures, please return to DIT Information Security Staff located in Virginia Square, Room Number 7067.

**Agency:** **Federal Deposit Insurance Corporation (FDIC)**

**System Name:** **TeamMate Audit Management System**

**System Acronym:** **OIG TeamMate**

**System Owner/Division or Office:** **FDIC OIG Office of Audits**

### **A. Information and Privacy**

To fulfill the commitment of the FDIC to protect personal data, the following requirements must be met:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual's privacy rights.

Given the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the FDIC, to share sensitive personal information.

## **B. Contact Information:**

1. Who is the person completing this PIA?

Name: Julio Santos, Jr.  
Title: Audit Specialist  
Organization: FDIC OIG, Office of Audits  
Contact Information:  
Address: 3501 N. Fairfax Drive, Arlington 22226  
Telephone number: 703-562-6347

2. Who is the Program Manager for this system or application?

Name: Julio Santos, Jr.  
Title: Audit Specialist  
Organization: FDIC OIG, Office of Audits  
Contact Information:  
Address: 3501 N. Fairfax Drive, Arlington 22226  
Telephone number: 703-562-6347

3. Who is the Project Manager for this system or application?

Name: Eugene Szczenski  
Title: Senior Information Technology Specialist  
Organization: FDIC OIG, Office of Management and Congressional Relations  
Contact Information:  
Address: 3501 N. Fairfax Drive, Arlington 22226  
Telephone number: 703-562-6301

4. Who is the IT Security Manager for this system or application?

Name: Richard Lowe  
Title: OIG Information Security Manager  
Organization: FDIC OIG  
Contact Information:  
Address: 3501 N. Fairfax Drive, Arlington 22226  
Telephone number: 703-562-6302

5. Who is the Chief Privacy Officer or designee who reviewed this document?

Name: Michael Bartell  
Title: Chief Information Officer and Director  
Organization: Division of Information Technology  
Contact Information:  
Address: 3501 N. Fairfax Drive, Arlington, VA 22226  
Telephone number: 703-516-5781

## **C. System Description**

This section of the Privacy Impact Assessment (PIA) describes the application and the method used to collect, process, and store information. Additionally, it includes information about the business functions the system supports.

Overview of the TeamMate Application:

The TeamMate application is a commercial off-the-shelf information system supporting the OIG's audit/evaluation responsibilities set forth in the Inspector General Act of 1978, 5 U.S.C. App. 3. The system is maintained to increase the efficiency and productivity of the audit/evaluation process by automating working paper preparation, internal review and retention. The system utilizes the commercial software product, TeamMate, to manage and integrate working papers prepared with various standard office automation products.

## **D. Data in the System**

1. What personal information about individuals or other information that can personally identify an individual (name, social security number, date of birth, address, etc.) is contained in the system? Explain.

The system is used in conducting audit/evaluation work of the Federal Deposit Insurance Corporation's programs and operations and in preparing related reports on behalf of the OIG. TeamMate documents the audit process – planning preparation, review and storage – in an electronic format. The nature and scope of the information is determined by the objectives of the audit/evaluation. Therefore, the information pertaining to a specific audit/evaluation may or may not contain personally identifiable information. Furthermore, the nature of any personally identifiable information will vary depending on the circumstances of the audit/evaluation, although such information is typically not included in this system. To the extent that personally identifiable information is collected, it is generally maintained in the audit/evaluation work papers and not disseminated to the public or readers of the related reports.

2. Can individuals “opt-out” by declining to provide personal information or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

No. OIG employees and contractors are required to cooperate with OIG activities. However, personal information is typically not collected from individuals in the course of audits and evaluations. If such information were collected, the individual would not have the right to consent only to a particular use.

3. What are the sources of the information in the system? How are they derived? Explain.

Information contained in this system consists of documents and data requested from, and the results of discussions with, agency and non-agency sources. Information in the system is derived from discussions with agency and non-agency sources, as well as analyses done by Office of Audit (OA) employees, contractors, and other staff. OIG has a statutory right to agency information and has statutory authority to subpoena records from non-federal entities.

4. What Federal agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

If deemed necessary and depending on the type and scope of an audit/evaluation, the OA could obtain such data on individuals or entities from other Federal agencies. The purpose in collecting that data would be to obtain information that is relevant to the audit objectives. Relevant data would be used, as appropriate, in conducting audit work and preparing related audit reports and other documents.

5. What state and local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

If deemed necessary and depending on the type and scope of an audit/evaluation, the OA could obtain such data on individuals or entities from state and local agencies. The purpose in collecting that data would be to obtain information that is relevant to the audit objectives. Relevant data would be used, as appropriate, in conducting audit work and preparing related audit reports and other documents.

6. What other third party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.

If deemed necessary and depending on the type, objective, and scope of an audit/evaluation, the OA could obtain such data on individuals or entities from other third party sources. The purpose in collecting that data would be to obtain information that is relevant to the audit objectives. Relevant data would be used, as appropriate, in conducting audit work and preparing related audit reports and other documents.

## **E. Access to Data:**

1. Who will have access to the data in the system (e.g., users, managers, system administrators, developers, contractors, other)? Explain their purpose for having access to this information.

Access to any FDIC OIG audit information is based on a business need to know. Only authorized staff conducting or reviewing audits/evaluations use TeamMate. Access to information for individual audits is limited to staff assigned to the audit/evaluation. Other offices within the OIG, such as the Office of Investigations or the Office of Counsel to the Inspector General, may have a need on a case-by-case basis to review audits/evaluations conducted using TeamMate. Other law enforcement agencies may be provided the information based on the scope and findings of an audit/evaluation; information may also be shared with auditees and other third parties when necessary to obtain information relevant to the audit/evaluation. The OIG's audit/evaluation process is subject to a quality control review conducted by the Inspector General of another agency. Information in Teammate may be viewed during such a quality control review. A limited number of DIT LAN Management system administrators also have access to the Teammate application for the purpose of supporting hardware and network services.

2. How is access to the data determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Explain the process.

Access to Teammate is role-based according to job function and contingent on a business need to know. All users must have the approval of OIG Office of Audits management to gain access to the system. The criteria, procedures, controls and responsibilities regarding access are found in Office of Audits policy and/or the application system documentation ("TeamMate Functional Overview" and "TeamMate Suite IT Overview").

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

Generally, users have limited access to the system which allows them to see only the information specific to the audit/evaluation to which they are assigned. Certain supervisory personnel have broader access privileges.

4. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access? (Please list processes and training materials) Explain the controls that have been established and how are they monitored or reviewed.

TeamMate has controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, network permissions, and software controls. Additionally, TeamMate users are required to complete FDIC's Corporate Information Security Awareness Training and Privacy Act Training on an annual basis.

5. Do other systems share data or have access to the data in the system? If yes, explain the purpose for the need to have access.

No

6. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface? Has policy or procedures been established for this responsibility and accountability? Explain.

N/A. Please refer to question #E.5 above.

7. If other agencies use the data, how will the data be used? Who establishes the criteria for what data can be shared? Have non-disclosure agreements been effected? Explain the purpose for the need to share the data?

N/A

8. Who is responsible for assuring proper use of the data? Is this individual fully accountable should the integrity of the data be compromised? Explain.

The Data Owner, Program Manager, and individual application users are responsible and accountable for assuring proper use of the data. OIG Policies and Procedures Manual Chapters 110.7, Chapter 110.9, Chapter 340.5, Chapter 370.4, and Chapter 300.1 in the provide the OIG policy for releasing information and reports to the public, the media, and the Congress.

9. Explain the magnitude of harm to the corporation if privacy related data is disclosed, intentionally or unintentionally. Would the reputation of the corporation affected?

As stated above, very little privacy related information is maintained in TeamMate. Therefore, the risk of harm to the FDIC would be low. However, if privacy related data in the system were intentionally or unintentionally disclosed, it is possible that the FDIC's reputation could be adversely affected

10. What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

The TeamMate application is a commercial off-the-shelf application. The manufacturer has no access or involvement with maintaining the actual information contained in the database. The manufacturer provides product version updates that the application owner is responsible for loading. Technical support for the application is provided by the manufacturer; however, the support provided only pertains to the functionality of the application.

11. Explain whether or not the data owner is contacted if it is not clear if other agencies share or have access to the data.

N/A

#### **F. Accuracy, Timeliness, and Reliability**

1. How is the data collected from sources other than FDIC records verified? Has action been taken to determine its reliability that it is virus free and does not contain malicious code? Who is responsible for this making this determination? Explain.

N/A

2. How will data be checked for completeness? How is this being measured? What is the source for ensuring the completeness of the data? Explain the method used.

N/A

#### **G. Attributes of the Data?**

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? Is this part of the system design? Is this documented, if so, where is the document located? Explain.

The information collected in Teammate is relevant and necessary to support the functional requirements of the application. Its use is part of the system design and is documented in the system documentation provided by the system's manufacturer.

2. Will the system derive personal identifiable information from the any new data previously non-inclusive, about an individual through aggregation from the information collected? What steps are taken to make this determination? Explain.

The TeamMate application is not intended to, nor is it programmed to, determine whether personal identifiable information can be derived through the aggregation of information collected. Users, through reviewing the collected information, would have to make this determination. The determination would be based on the judgment of the user.

3. Can the system make privacy determinations about employees that would not be possible without the new data? If so, explain.

The TeamMate application is not intended to nor is it programmed to determine whether personal identifiable information can be derived through the aggregation of information collected. OIG assignment team members, through reviewing the collected information, would have to make this determination. The determination would be based on the judgment of the assignment team members.

4. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Does the consolidation of data result in personal identifiable information? Explain.

See Section E. Access to Data, for the controls on access to a TeamMate file and data.

5. How is the data retrieved? Can it be retrieved by a personal identifier (e.g., social security number)? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

TeamMate offers limited Search and Retrieve capabilities. Full text searching is available on any text field of a TeamMate form based on a word or phrase. Teammate does not allow text searches over numerous individual workpapers and does not provide for the retrieval of information using any type of personal identifier.

6. What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them? Explain how they are distributed.

None.

## **H. Maintenance and Administrative Controls:**

1. If the system is operated in more than one site, how will consistent use of the system and data are maintained in all sites? Will the same controls be used? Explain.

The TeamMate application is operated at more than one site as an on-line database application. All application security controls apply at each site.

2. What are the retention periods of data in this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? Explain.

The retention period for data in this system is generally ten years as set forth in Chapter 130.3 - Records Disposition Program of the OIG's Policies and Procedures Manual. See also, H.3

3. What are the procedures for disposition of the data at the end of the retention period? How long will any reports produced be maintained? Where are the procedures documented? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the procedures? Explain.

The procedures for the disposition of the data in and associated with this system are set forth in Chapter 130.3 - Records Disposition Program of the OIG's Policies and Procedures Manual. The manner of disposing TeamMate records has not been determined. This determination will depend on expected future guidance from legislation or from the National Archives and Records Administration. Until that determination is made, TeamMate records may be retained indefinitely.

4. Is the system using technologies in ways that the Corporation has not previously employed (e.g., Monitoring software, SmartCards, Caller-ID, biometrics, PIV cards, etc.)? Explain.

N/A

5. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology? Explain.

The use of the TeamMate application should have no perceptible affect on privacy. Any privacy related information is included in the system only if relevant to the objectives of an audit or evaluation. Any privacy related information in reports or related documents would not, in general, be publicly released. Moreover, personally related information cannot be retrieved from the system by personal identifier.

The use of this technology does not introduce the risk of compromising the integrity of privacy related information in the system when compared to information maintained in hardcopy files. In fact, the use of technology may reduce the risk of compromise in that paper records may be easier to review than a series of computer screens

6. If monitoring is being performed, describe the data being collected. Is monitoring required? If so, describe the need for the monitoring and identify the requirements and explain how the information is protected.

There is no monitoring of individuals.

7. If monitoring is not required, explain the controls that will be used to prevent unauthorized monitoring?

The system is not used to monitor individuals. The system is only accessible by those OIG employees who have been authorized and then only for selected information on a need to know basis.

8. In the Federal Register, under which Privacy Act Systems of Record (SOR) does this system operate? Provide number and name.

N/A

9. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

N/A

## **I. Business Processes and Technology**

1. Does the conduct of this PIA result in circumstances that requires changes to business processes?

No.

2. Does the completion of this PIA potentially result in technology changes?

We are not aware if the manufacturer of the TeamMate product is contemplating any changes to their product based on the sensitive information issues.